Maryland Auditing and Compliance Policy

Last Updated: 05/30/2017

Contents

1.0 Purpose

The Maryland Department of Information Technology (DoIT) is responsible for, and committed to, managing the confidentiality, integrity, and availability of State government information technology (IT) networks, systems, and applications within the scope of its authority.

To accomplish this, DoIT must audit State-owned assets, ensure secure configurations are used, manage change across the network, and discover vulnerabilities within the IT architecture. Essentially, DoIT must identify what risks are present and act to mitigate or eliminate those risks to protect the network and systems from compromise or data loss. To help ensure a secure network, it is crucial to determine whether the network, systems, and practices comply with policies, regulations, laws, directives, and orders.

This policy outlines the requirements of implementing an **information assurance** function within the DoIT cybersecurity program. DoIT will utilize the baseline controls and standards established by NIST SP 800-12, SP 800-30R1, 800-36, 800-37R1, 800-39, 800-47, 800-50, and 800-53R4.

2.0 Document and Review History

This policy supersedes the Maryland Information Security Policy v3.1 (2013), Section 5.0: Management Level Controls; Section 6.0: Awareness and Training; Section 6.7: System and Information Integrity; Section 7.1: Audit & Accountability Control Requirements; and Section 13: Data Loss Prevention Guidance and any related policies declared prior to the 2017 Cybersecurity Program Policy. This document will be reviewed annually and is subject to revision.

Date	Version	Policy Updates	Approved By:
01/31/2017	v1.0	Approval of Draft	Maryland CISO
05/30/2017	v1.1	Initial Publication	Maryland CISO

3.0 Applicability and Audience

This policy is primarily applicable to the DoIT Enterprise and establishes the requirements for appropriate auditing within the Enterprise to ensure agency compliance to the overall *DoIT Cybersecurity Program Policy* and its supporting policies. Agencies under the policy authority of, but not directly managed by, DoIT will be responsible for independently implementing Section 4.0 and the requirements as indicated within each sub-section.

4.0 Policy

As directed under 2013 Maryland Code § 3A-303 and 3A-305, DoIT is consolidating the IT infrastructure of Maryland Executive Branch agencies. This consolidation aims to standardize hardware and software security and operational requirements to create effective and efficient processes, procedures, and services across the multiple agencies comprising this Enterprise. An inherent part of this Auditing and Compliance policy is to identify and mitigate agency-based

risk. While agencies are considered the data owners and are responsible for ensuring processes and procedures are in place to protect data and prevent unauthorized access, it is DoIT's mission to ensure cohesive security across the State of Maryland's IT infrastructure.

To adequately protect information and the systems that process it, the State CISO will appoint an Enterprise **Information System Security Manager (ISSM)** who reports directly to the State CISO and will be responsible for enforcing cybersecurity program policies and for providing network, system, and process auditing to ensure compliance with established policies, regulations, laws, directives, and orders. The ISSM will assist the **Enterprise Risk Manager** with identifying, assessing, and mitigating risk within the Enterprise and with assuring the protection of confidential information. The following subsections describe the requirements for implementing an information assurance capability within the Enterprise.

4.1 Cybersecurity Program Auditing

The Enterprise ISSM, or delegated staff, will conduct information technology security audits of Enterprise onboarded-agency assets. The Enterprise ISSM will develop an audit plan to ensure all onboarded assets and processes are compliant with active DoIT security policies.

Agency data-owners and agency IT staff will coordinate with the Enterprise ISSM by gathering data, reviewing existing policies and processes, and reporting to agency management. All Agency Security Managers (see *DoIT Agency Security Incident Management Plan*) will provide audit results to the State CISO along with any recommended changes or remediation.

Agency Security Managers will work with the Enterprise ISSM to develop agency-based security audit plans. This will ensure consistent auditing procedures are followed and audits are completed within an acceptable timeframe. The core requirements for this plan are listed in the table below.

#	Name	Requirement
A	Security Audit Plan	List each agency to be audited, identify what audits will be conducted, and when (e.g., first calendar quarter).
B	Agency Inventory and Configuration	Ensure an annual asset inventory and configuration report, including approved changes, is available. All assets should be accounted for and any deviation from the previous configuration report should have been recorded in the change control process.
C	Policy and Process Review	▪ Review Enterprise policies yearly to ensure any policy changes or agency requirements are identified and incorporated into the security audit ▪ Review processes for accuracy and policy compliance and update them in coordination with IT administrators and security staff to reflect any hardware, software, or process changes ▪ Ensure agency audits assess IT staff compliance with established processes
D	Audit Schedule	Schedule audits to review each agency's assets and processes within an acceptable interval (e.g., every three years). This schedule may change due to new agencies onboarding to the Enterprise, but "new" audits should be completed within a reasonable time.
E	Previous Audit Results	Review previous audit results for action items, notes, or policy exemptions to ensure each agency assessment is continuous and progressing toward security goals.

#	Name	Requirement
F	Audit Results	Analyze audit results to determine overall compliance and identify action items or improvements. The results will be provided to the agency management for remediation and to ensure management is aware of the agency's level of compliance.
G	Reporting	Report the agency's audit results to the State CISO. For any agency not compliant with a policy or clearly violating a policy requirement, the CISO may report to the Secretary of Information Technology for remediation as indicated within Section 8.0: Enforcement of each policy.

4.1.1 Office of Legislative Audits Review

The Enterprise ISSM will coordinate with the Office of Legislative Audits (OLA) to ensure DoIT management establishes and maintains effective internal controls. Per OLA, internal control is a process designed to provide reasonable assurance that objectives pertaining to the reliability, effectiveness, and efficiency of operations are achieved, including the safeguarding of assets and compliance with applicable laws, rules, and regulations.

The Enterprise ISSM will ensure that control of information security documentation and comprehensive record keeping are implemented and managed within DoIT and the onboarded agencies. The ISSM will also ensure existing policies are updated per the Security Audit Plan and that both the policies and the Security Audit Plan are available to the OLA auditors for review.

4.1.2 Security Operation Center Coordination

During investigations of suspicious cyber events such as anomalous user behavior or potential data breaches, the Security Operations Center (SOC) will coordinate with the Enterprise ISSM to oversee compliance with regulatory, policy, and privacy requirements. The ISSM will ensure proper forensic evidence collection and will interface with Human Resources and Legal Counsel, as needed. Policies will be reviewed during the incident response evaluation phase and updated to ensure the security posture of the IT infrastructure is maintained while adapting to new and evolving threats. The ISSM will also work with the Director of Security Operations to document the actions and outcome of the incident, including ensuring proper closure and management notification.

The Enterprise ISSM will ensure SOC monitoring activities do not violate existing privacy laws and regulations and will audit SOC operations periodically to ensure compliance. Within the scope of routine monitoring and during investigations, the SOC may collect or be exposed to private user information, such as privileged communications between client-attorney, doctor-patient, or clergy-communicant. The ISSM will work with SOC analysts to ensure any breach of these privileges are properly documented and reported.

4.2 Risk and Vulnerability Analysis

The Enterprise ISSM will coordinate with the DoIT Risk Manager to identify security risks to the information technology infrastructure and the **confidential data** handled within the Enterprise. The ISSM will use targeted, qualitative risk assessments to prioritize risks and help

identify cost effective risk reduction. This will allow the ISSM and Risk Manager to perform **threat modeling**, such as the CIS Community Attack Model, which uses known attack vectors to identify risks with the biggest impact to the organization.

The ISSM is responsible for analyzing vulnerabilities within the infrastructure and assessing overall patch compliance. ISSM vulnerability-scan audits will verify systems are being patched according to schedule and patch criticality (see *Patch Management Policy*).

4.2.1 Network Connection Review

Agencies and third parties requesting an Authority to Operate (ATO) or a Third Party Interconnection Agreement will be required to submit a request package that includes the System Security Plan (SSP), assessment supplements, and plan of actions and milestones to the ISSM for review (see *Cybersecurity Authority to Operate Policy* and *Third Party Interconnection Agreement Policy*, respectively). The ISSM will analyze the package to determine risks associated with the connection and ensure mitigation strategies are in place to reduce or eliminate any identified threats.

The ISSM will work closely with the Designated Approval Authority (DAA) to help determine an acceptable level of risk relative to identified vulnerabilities before the DAA authorizes any connections to DoIT's infrastructure.

4.2.2 Information Assurance

The Enterprise ISSM is responsible for maintaining information assurance, utilizing data loss prevention (DLP) tools and enforcing data classification requirements to ensure that confidential information can be identified, protected, and tracked within the Enterprise. The ISSM will coordinate with the SOC to monitor possible security violations and recommend security improvements.

Agency ISSMs will be required to oversee the review of any DLP audit logs and files to ensure that confidential data is not inadvertently disclosed, putting the agency at risk of a data breach.

Agencies will be accountable and responsible for properly classifying and protecting their information. For onboarded agencies, the ISSM will periodically review audit logs and monitoring tools related to data access and transfers to identify potential data loss or compromise.

4.3 Asset and Configuration Coordination

The ISSM will coordinate with asset managers to ensure all Enterprise IT assets are accounted for, properly tracked, and any discrepancies are investigated to determine if a security violation exists.

Agency asset managers will conduct yearly inventories as directed in the DoIT *Asset Management Policy* and provide inventory results to the ISSM for review. Assets with data storage capabilities designated for disposal will be reviewed by the ISSM to ensure data is properly removed.

The ISSM will ensure each agency's IT assets have configurations that support the mission and business of the agency and meet security requirements to protect from data loss or compromise. Asset configurations will be maintained by the agency configuration manager as directed in the DoIT *Configuration Management Policy*, and unauthorized changes will be reported to the ISSM for investigation. The ISSM may determine whether an unauthorized change is a security violation and will report violations to the SOC for investigation and mitigation.

4.4 Change Control Board

As indicated in the *Configuration Management Policy (see section 4.1)*, the ISSM is a member of the Change Control Board (CCB) to ensure security is implemented properly in all information technology change requests. This effort enables agencies to integrate changes efficiently and ensures security components are adapted to the implemented solutions.

The ISSM will be notified of pending change requests and will conduct technical reviews to proposed IT product procurements, configuration changes, or other technical solutions to ensure compliance with security policies and procedures and to determine potential changes to the existing security posture to accommodate the requested change.

The ISSM will be responsible for ensuring proposed changes do not adversely affect the security of the IT infrastructure and for determining measures to mitigate exposed risks or vulnerabilities caused by the change. The following table identifies typical criteria to consider before introducing any change to the inventory, configuration, or processes currently in effect. This list is not all-inclusive and will vary depending on the proposed change and the network or systems affected.

#	Name	Requirement
A	Identify Risk	Determine any known threats against the proposed change and the vulnerabilities the change could create.
B	Determine Asset Adaptation	Obtain approval to use any new asset on the network after a risk analysis and security review.
C	Identify Security Configuration Changes	Determine if any ports, protocols, or connections must be opened, enabled, or attached to devices such as firewalls or POTS modems (such as required by certain network attached storage vendors).
D	Identify Changes in Services	Determine whether new devices or systems require insecure services to be installed or enabled, (e.g., old, unencrypted versions of Simple Network Management Protocol (SNMP)).
E	Review Security Requirements	Work with change requestors to determine secure solutions to proposed changes that incur risks to the infrastructure. Resolve concerns such as manpower required to maintain and operate a new system; locations for new assets; support requirements (e.g., log aggregation and security configuration); and logical changes to the network.

4.5 New Hire Training and Awareness

The Enterprise ISSM will develop a new-user, information-security training package that will be available to agency support staff at onboarding and at any new-account creation. The package will meet the requirements identified in the table below.

#	Name	Requirement
A	Identify Accessible Training Medium	The training package must be readily accessible by users before first logon to ensure the new user is aware of and accountable for understanding and accepting DoIT information security policies. This medium may be paper based, such as a printed presentation binder, a video or slideshow format, or other medium a new user can access before logging in to the network.
B	Protect Confidential Information	Define the user's responsibility to protect confidential information and how to report possible information compromise, including inadvertent disclosures.
C	Protect User Accounts and Systems	Inform users of account security requirements, such as password size, complexity, and constraints; restrictions on sharing accounts; locking unattended systems; etc. (see *Account Management Policy*)
D	Threat Awareness	Inform users of the current threat landscape and typical mitigations, for example, identifying common spam and phishing attacks and common social engineering methods. This training should include instructions on operational security (OPSEC) concerns and best practices for protecting the user's own information.
E	Issue Reporting	Inform users of who to contact for security concerns, technical issues, and other important contact information, such as dialing for emergency services.
F	Acceptable Use Policy	▪ Require new users to read the DoIT *Acceptable Use Policy* and sign the user acknowledgement form located in Appendix A; any user receiving a privileged account must also sign the Privileged User form in Appendix B ▪ Support staff will collect the signed acceptable-use form and provide the user credentials to log on to the network; once collected, the forms will be provided to the ISSM as evidence of the user's understanding of DoIT security practices ▪ The ISSM will maintain records of user training and will coordinate with the agency Human Resources department to ensure the signed forms are included in personnel records

Yearly Campaign

The Enterprise ISSM will also establish an annual information security training and awareness initiative for all onboarded agency staff (State employees and contractors). The requirements for the training and awareness campaign are listed in the table below.

#	Name	Requirement
G	Schedule	Schedule multiple sessions of training in advance to ensure maximum attendance by agency staff while keeping session headcount to a reasonable level.
H	Attendance Tracking	Record all users attending training events (e.g., provide a "sign-in" sheet and make sure all who attend sign in).
I	Reporting	Provide users with information on how to report security infractions or incidents (e.g., losing a mobile device), as well as current contact information for agency security and technical functions.
J	Security Practices and Changes	Ensure users understand current security practices, and introduce any near-term changes that may impact users.

#	Name	Requirement
K	Current User-Related Threat Environment	Coordinate with the SOC to present information on current and popular types of attacks users may encounter as well as advice for protecting personal information and devices.
L	User Policy Updates	Inform users of any changes to relevant policies or services, i.e., changes to the acceptable use policy or to browser whitelists or blacklists.
M	Acceptable Use Form	▪ Require users to sign an acceptable-use form each year to ensure user accountability and responsibility for protecting the systems and information they access ▪ The ISSM will track attendance at user security and awareness sessions along with a record of signed, updated Acceptable Use forms; the ISSM will coordinate with Human Resources to ensure signed and updated forms are entered into personnel records
N	Attendance Verification	The ISSM will ensure attendance rosters match collected, signed acceptable-use forms and that all staff have attended annual information security training.

5.0 Exemptions

This policy is established for use within the DoIT Enterprise. If an agency under the policy authority of DoIT requires an exemption from this policy, then that agency must submit a DoIT Policy Exemption Request Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks and the agency's mitigation strategy associated with this exemption. If the agency can accept the risk, an exemption to this policy may be granted.

6.0 Policy Mandate and References

The Cybersecurity Program Policy mandates this policy. Related policies include:

- Acceptable Use Policy
- Account Management Policy
- Agency Security Incident Management Plan
- Asset Management Policy
- Configuration Management Policy
- Cybersecurity Authority to Operate Policy
- Continuous Monitoring Policy
- Patch Management Policy
- Public and Confidential Information Policy
- Security Assessment Policy
- Third Party Interconnection Agreement Policy

7.0 Definitions

Term	Definition
Confidential Data	Confidential information is non-public information that, if disclosed, could result in a negative impact to the State of Maryland, its employees, or citizens and includes the following sub-categories: ▪ Personally Identifiable Information; ▪ Privileged Information; and ▪ Sensitive Information For more information on confidential information see *DoIT Public and Confidential Information Policy.*
Enterprise Risk Manager	Position responsible for the management and enforcement of the Risk Assessment requirements described in the *DoIT Security Assessment Policy*.
Information Assurance (IA)	Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.
Information System Security Manager (ISSM)	Individual responsible for the information assurance of a program, organization, system, or enclave.
Threat Modeling	Systematic process of anticipating an attacker's behavior by identifying and rating objectives and vulnerabilities of a network to determine mitigation strategies and protect against various threats.

8.0 Enforcement

The Maryland Department of Information Technology is responsible for enforcing policies for Enterprise onboarded agencies. The DoIT Cybersecurity Program identifies the minimum requirements necessary to comply with the information security standards and guidelines provided within Cybersecurity Program Policy and its supporting policies. Agencies not directly managed by DoIT must exercise due diligence and due care to comply with the minimum standards identified by the relevant DoIT policies.

If DoIT determines that an agency is not compliant with this policy or any supporting policy, the non-compliant agency will be given a sixty (60) day notice to become compliant or at least provide DoIT a detailed plan to meet compliance within a reasonable time before the issue is reported to the Secretary of Information Technology. After which, the Secretary of Information Technology, or a designated authority, may extend a non-compliant agency's window of resolution or authorize a DoIT representative to limit or restrict an agency's access to external and internal communications (effectively shutting down connectivity) until such time the agency becomes compliant.

Any attempt by personnel to circumvent or otherwise bypass this policy or any supporting policy will be considered a security violation and subject to investigation and possible disciplinary action, which may include written reprimand, suspension, termination, and possible criminal and/or civil penalties.